Hybrid Warfare Research Institute

Udruga Sv. Jurja St. George Association

Hybrid Threats and Resilience of Society, Critical Infrastructure, and the State

7 Zagreb Security Forum 2022

7-8 October 2022, Zagreb, Croatia

Concluding Findings and Remarks

1. There is a strong change of attitudes and threat perceptions throughout Europe relating to national and regional security and stability. Much of this change has certainly been brought about by the Russian invasion of Ukraine, but it was also influenced by the strong sense of insecurity caused by the corona pandemic crisis.

2. There is a clear focus on NATO as the central pillar of European security. This is a stark change in the position of many people in Europe that, only a few years ago, claimed that NATO lost its role in the security of Europe and should be disbanded. Existing security architecture where NATO is in core of it proved its reason to exist especially in the context of Russian aggression on Ukraine.

3. There is a wider involvement of government and civil society entities in security policy formulation and implementation in Europe and beyond. In the past, security policy was a well-defined, limited arena in which the principal actors were defence ministries and the military. Now, with the realisation of hybrid warfare as a major threat, security requires a whole of society approach for defending freedom and democracy. Security become measure of resilience against emerging security challenges.

4. Hybrid warfare has become the norm rather than the exception. Until recently, hybrid warfare was considered by many to be a peripheral, even arcane, type of warfare. The Russian invasion of Ukraine and the ensuing hybrid attacks clearly illustrates

This workshop is supported by: The NATO Science for Peace and Security Programme

that hybrid warfare is now an integral and central part of interstate conflict. Just as future conflicts and wars between different players.

5. Critical infrastructure is becoming a key target for hybrid warfare. Its vulnerabilities will further expand by the energy crisis. Energy infrastructure is large, diffused, and difficult to protect. It is rapidly becoming not only a sensitive lifeline of societies and economies but also the target for well-planned potential hybrid warfare attacks. Therefore, we need to adopt present thinking of Critical infrastructure protection. We need to focus our efforts to define key critical infrastructure (KCI) that needs to be specially protected. Key critical infrastructure can be defined as a critical infrastructure that functionality of other critical infrastructures relies most on them, and that malfunction of KCI can have a significant negative cascade failure impact to other CI.

6. Russian hybrid threats and their malicious influence to societies and population of NATO allies is significant. The intention is to create social divisions, ruptures that hybrid attacker will use for its purposes. Strengthening democracy, protecting freedom and society, and increasing the societal resilience against hybrid threats needs to be one of the basic pillars of security and safety in NATO allies and EU member states.

7. Hybrid risks and threats analysis needs to be written on national and level of organizations such as NATO and EU. We saw many examples on ZSF 2022 that activities that, at first sight looks like usual commercial, financial, and social activities have a completely different background and intentions that might lead to future malicious hybrid activities by hybrid attacker.

8. The shifting national priorities towards defence expenditure will be curtailed by inflation and economic crises. The current aim of many NATO member states of reaching a level of defence expenditure at 2% of GDP will be difficult to achieve as the economic crisis deepens and inflation forces reductions in public spending.

This workshop is supported by: The NATO Science for Peace and Security Programme

Closer European coordination and integration in defence and security, as well as closer cooperation with Europe's allies such as Israel, can achieve substantial savings in defence expenditure while at the same time enhancing your overall military capabilities and its defence posture.

9. One of the key answers for developing social and state resiliency against hybrid threats is in scientific cooperation between various partners and experts on national and international level. Without investments in research and development, multidisciplinary approach to emerging security challenges, integration of knowledge, without creation of international network of experts and ability to exchange information and knowledge, it will be very hard to recognize early enough signals of coming hybrid threats. We need to shift the focus of scientist to make deep and substantial research on risks that have a low probability of their appearance but high impact by its possible negative consequences.

10. Risk of using weapons of mass destruction (WMD) in Russian aggression on Ukraine in 2022 was/is an argument with which Russia, obviously, tried to obtain better position for itself in negotiations that will start in one moment. It looks like that the risk of using WMD, especially nuclear weapons, as a one of the vectors of malicious attack, proved to be a highly risky move for the attacker. Russian possible intentions to be the first one that might use the WMD in Ukraine, was faced with significant negative attitude and reactions in international community. Existing security architecture is, until now, enough to prevent usage of WMD by deterring it with threats of counterattack using combination of modern weapons supported by massive cyber-attacks within and outside of cyber domain.

NATO OTAN — This workshop is supported by: The NATO Science for Peace and Security Programme